1.物理机不要有任何黑客行为的操作，如果你以前常用物理机进行黑客活动，那么，重装系统，备份敏感资料，其余的不要保存，对整个磁盘格式化重新分区
2.重新安装好系统后，把补丁打全！随后安装虚拟机
3.建议安装2个虚拟系统，A用来做众测之类的渗透，B用来做敏感的渗透
4.虚拟机中的系统与浏览器不要使用本国语言（安装系统时，同时建议安装好后不要安装本国语言）
5.使用NAT！！！
6.开启防火墙并在入站连接里对139、445端口禁止连接（物理机同样开启）
7.不要安装杀软
8.安装防火墙软件，发现可疑连接立即阻止，不要尝试允许
9.不要使用IE浏览器
10.虚拟机中的系统不要安装本国输入法，最好使用自带输入法，毕竟你不可能经常使用
11.将虚拟机中的系统补丁全部安装
12.不要安装任何国产软件和网民常用软件
13.不要安装任何带有国家性质的程序，如中文程序
14.虚拟机中不要使用百度、有道等国内翻译网站
15.如果虚拟机中的软件提示更新，不要进行更新，关掉后去官网下载最新版本
使用比特币购买VPS

使用比特币购买VPS，禁止使用支付宝、淘宝、PayPal等实名认证的第三方支付

经调研目前购买比特币几乎都需要实名认证，如果实在找到不到可以不实名购买的站点，则先创建两个比特币钱包，去网站购买比特币，汇入其中一个钱包地址，在实名认证后，如果可以，注销删除掉你购买比特币时实名认证的的账户，如果不能删除，则谨慎二次使用，随后去A网洗比特币的站点进行混淆，混淆后，汇入另外一个钱包中，在去支持比特币支付的站点购买VPS，建议购买两台，一台用来做众测之类的渗透，另外一台用来做敏感的渗透。

购买后，不要使用自己真实地址连接，如果可以，去H掉一台服务器，如果是windows，创建vpn，再进入虚拟机中使用vpn拨号的方式连接你的VPS，建议VPS同时搭建vpn，先拨号H掉的，在拨号你自己的VPS（强烈建议2层VPN），如果是linux，不想使用vpn的情况下，可以使用如下方法(不推荐)
Proxifier+xshell转发应用程序请求(不建议使用)
//以下内容为以前编写，所以为中文
在你H掉的那台linux上创建个可疑远程ssh的账号或搭建socks5代理，并设置密码，禁止日志记录
安装xshell、Proxifier

关于2层VPN的设置（强烈建议）

1层VPN相当于没有，可以获取你的真实IP，为了防止个人真实IP泄露，强烈建议实行下面的建议
在虚拟机中先拨H掉的，在拨你匿名购买的，连接之前，使用如下设置方案
1、 VPN断开后，立即断开该虚拟机连接
2、 禁止断线重连
3、 实现方法如下，因本人使用的方法无法外泄，所以下面的方案网上找的，可行性自行实验
需要分三步对防火墙进行设置：

1. 默认阻止所有出口流量
2. 在本地连接上设置允许通向VPN服务器的出口流量
3. 允许所有流量通过vpn链接出去

操作系统层面的防护

网络层防护已经做得差不多了，下面是操作系统方面的防护，物理机与虚拟机建议同样设置为如下方案

禁用远程注册表服务，打开服务管理，找到显示名字为RemoteRegistry的服务，右键属性，禁用

禁用Server服务，如上面的方法找到后禁用

禁用NetBIOS,位置：网络连接-连接属性-ipv4-高级-wins-NetBIOS设置-禁用

开启防火墙，安装防火墙软件

禁用计划任务，方法自己找

计算机名称设置为随机字符串，不要asdf之类的